Cyclic Systems of Simultaneous Congruences

Jeffrey C. Lagarias
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109-1109
lagarias@umich.edu

(September 27, 2008)

Abstract

This paper considers the cyclic system of $n \geq 2$ simultaneous congruences

$$r\left(\frac{\prod_{k=1}^{n} q_k}{q_i}\right) \equiv s \pmod{|q_i|}, \quad 1 \leq i \leq n,$$

for fixed nonzero integers (r, s) with $r > 0$ and $(r, s) = 1$. It shows there are only finitely many solutions in positive integers $q_i \geq 2$, with $\gcd(q_1 q_2 \cdots q_n, s) = 1$ and obtains sharp bounds on the maximal size of solutions for almost all (r, s). The extremal solutions for $r = s = 1$ are related to Sylvester's sequence $2, 3, 7, 43, 1807, ...$ If the positivity condition on the integers q_i is dropped, then for $r = 1$ these systems of congruences, taken $(\mod |q_i|)$, have infinitely many solutions, while for $r \geq 2$ they have finitely many solutions. The problem is reduced to studying integer solutions of the family of Diophantine equations

$$r\left(\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}\right) - \frac{s}{x_1 x_2 \cdots x_n} = m,$$

depending on three parameters (r, s, m).

1. Introduction

Consider the cyclic system of n simultaneous congruences

$$\left(\frac{q_1 q_2 \ldots q_n}{q_i}\right) \equiv 1 \pmod{q_i}, \quad 1 \leq i \leq n, \tag{1.1}$$

to be solved in integers $q_i \geq 2$. Sequences $(q_1, ..., q_n)$ with $2 \leq q_1 \leq \cdots \leq q_n$ satisfying (1.1) were named *Giuga sequences* by Borwein et al. [2], who related such sequences to a conjecture of Giuga [7] on primality. For $n = 2$ there are no solutions to (1.1), but for $n = 3$ this system has the unique solution

$$\begin{aligned} 2 \cdot 3 &\equiv 1 \pmod{5} \\ 3 \cdot 5 &\equiv 1 \pmod{2} \\ 5 \cdot 2 &\equiv 1 \pmod{3}. \end{aligned} \tag{1.2}$$

For $n \geq 3$ this equation has the solution $(q_1, q_2, ..., q_n) = (u_1, u_2, ..., u_{n-1}, u_n - 2)$ where u_n are defined by the recursion $u_0 = 1$ and $u_{n+1} = (\prod_{i=1}^{n} u_i) + 1$. This sequence u_n starts

$1, 2, 3, 7, 43, 1807...$ and grows doubly-exponentially in n. It is often called *Sylvester's sequence*, after work of J. J. Sylvester [15] in 1880. (However in Knuth, Graham and Patashnik [8] this sequence is denoted e_n and its terms are called *Eulerian numbers*.) We show, as a special case of Theorem 1.1 below, that the solution above gives the maximal possible value of q_n in any Giuga sequence of length n.

In this paper we study solutions of the generalized system of cyclic congruences

$$r\left(\frac{q_1 q_2 \cdots q_n}{q_i}\right) \equiv s \pmod{q_i}, \quad 1 \le i \le n, \tag{1.3}$$

in which r, s are nonzero integers with $\gcd(r, s) = 1$, and we restrict to solutions satisfying the greatest common divisor condition $\gcd(q_1 q_2 \cdots q_n, s) = 1$. This gcd condition is equivalent to the q_k being pairwise relatively prime, as shown at the end of §2. Without loss of generality we reduce to the case $r > 0$ by multiplying the congruences by -1 if necessary; we allow s to be positive or negative. We also permit some variables $|q_i| = 1$, and call a solution nontrivial if at least two $|q_i| \ge 2$. We consider two situations: (1) the variables q_j are restricted to be positive integers; (2) the variables q_i are nonzero integers.

The following result shows there are finitely many nontrivial positive integer solutions to systems of simultaneous congruences (1.3) satisfying the gcd condition, and gives a bound on their size which is often sharp.

Theorem 1.1 *Let r, s be nonzero integers with $r > 0$ and $\gcd(r, s) = 1$. For each $n \ge 2$, there are only a finite number of solutions in positive integers $(q_1, q_2, ..., q_n) \in (\mathbb{Z}_+)^n$ to the cyclic system of n simultaneous congruences*

$$r\left(\frac{\prod_{k=1}^{n} q_k}{q_i}\right) \equiv s \pmod{q_i}, \quad 1 \le i \le n. \tag{1.4}$$

that satisfy the side conditions (i) at least two $q_i \ge 2$, and (ii) $\gcd(q_1 q_2 \cdots q_n, s) = 1$. Let the sequence $u_n(r)$ be given by $u_1(r) = r + 1$ and

$$u_{n+1}(r) = r\left(\prod_{i=1}^{n} u_i(r)\right) + 1. \tag{1.5}$$

Then each such solution to the cyclic system satisfies the upper bounds

$$\max\{q_i\} \le \begin{cases} \max\{u_n(r) - s - 1, s^2\} & \text{if} \quad s > 0, \\ \max\{u_n(r) - s - 1, |s|\} & \text{if} \quad s < 0. \end{cases} \tag{1.6}$$

For fixed r, s the upper bound $u_n(r) - s - 1$ is attained for all n having $u_n(r) > s^2$.

The case $r = s = 1$ covers the case of Giuga sequences. This theorem allows some moduli $q_i = 1$ to occur in the congruences; the corresponding congruence (mod 1) is then automatically satisfied. Such moduli can be eliminated, reducing the number of variables n to cases where all $q_i \ge 2$, retaining at least two such variables. The two side conditions on solutions are necessary for finiteness, because for $n = 2$, $r = 1$ and every $s \ge 1$, there are an infinite set of nontrivial positive solutions $\{(q_1, q_2) = (s, ks) : k \ge 1\}$. In Theorem 1.1 the case $s = 1$ is excluded by

side condition (i) that $q_1, q_2 \geq 2$, while all cases $s \geq 2$ are excluded by side condition (ii) that $gcd(q_1 q_2, s) = 1$.

The next two theorems concern solutions to (1.3) allowing positive and negative integers. An interesting feature here is that for certain parameter values there do exist exist infinitely many nontrivial solutions satisfying the side conditions (i),(ii). As an example, for $n = 3$ and $r = s = 1$ the values $(q_1, q_2, q_3) = (-k, k+1, k^2+k+1)$ for $k \geq 2$ are an infinite family of solutions. The following result shows that whenever $r = 1$ there are an infinite number of solutions.

Theorem 1.2 *Consider the cyclic system of n simultaneous congruences*

$$\frac{\prod_{k=1}^{n} q_k}{q_i} \equiv s \pmod{|q_i|}, \ , \quad 1 \leq i \leq n. \tag{1.7}$$

where s is nonzero.

(1) For each $n \geq 2$ this system has infinitely integer solutions $(q_1, q_2, \cdots, q_n) \in (\mathbb{Z} \setminus \{0\})^n$ with at least two $|q_i| \geq 2$ and

$$\gcd(q_1 q_2 \cdots q_n, s) = 1.$$

(2) For each $n \geq 2$ there exists an integer M_n^* such that when $\gcd(s, M_n^*) = 1$, this system has infinitely many integer solutions satisfying

$$\gcd(q_1 q_2 \cdots q_n, s) = 1 \quad \textit{and} \quad \min\{|q_i|\} \geq 2.$$

An allowable value is $M_n^* = u_1 u_2 \cdots u_n$, where $u_i = u_i(1)$ are terms in Sylvester's sequence.

In the second part of this result the proof determines the minimal values $M_2^* = 1$ and $M_3^* = 2$. It does not determine the minimal value for $n \geq 3$, but it might be that that the general minimal value is $M_n := gcd(2, n+1)$.

The next result shows that in the remaining cases $r \geq 2$ there are always a finite number of integer solutions, and obtains an upper bound on their size.

Theorem 1.3 *Let $r \geq 2$ and s be integers with $\gcd(r, s) = 1$. Then the cyclic system of n simultaneous congruences*

$$r\left(\frac{\prod_{k=1}^{n} q_k}{q_i}\right) \equiv s \pmod{|q_i|} \ , \quad 1 \leq i \leq n \ . \tag{1.8}$$

has only finitely many integer solutions $(q_1, q_2, \cdots, q_n) \in (\mathbb{Z} \setminus \{0\})^n$ having $\gcd(q_1 q_2 \cdots q_n, s) = 1$. All such solutions satisfy the bound

$$\max\{q_i\} \leq (r(n+1))^{2^{n-1}} + |s|. \tag{1.9}$$

The upper bound (1.9) is far from tight; a slightly better upper bound, more complicated to state, is given in Theorem 5.1. It might be that the upper bound of Theorem 1.1 actually gives the extremal bound for positive and negative variables, at least for n large enough (depending on r and$|s|$).

The proofs of Theorems 1.1-1.3 are based on reducing solutions of the cyclic congruences to solutions of a family of Diophantine equations depending on three parameters (r, s, m), namely

$$r\left(\frac{1}{x_1}+\frac{1}{x_2}+\cdots+\frac{1}{x_n}\right)-\frac{s}{x_1x_2\cdots x_n}=m, \tag{1.10}$$

In Lemma 2.1 we show that a cyclic congruence solution $(q_1, ..., q_n)$ satisfies (1.10) for some integer m, a fact noted by Borwein et al. [2]. The condition $\gcd(q_1q_2\cdots q_n, r|s|) = 1$ leads to a one-to-one correspondence of solutions $(q_1, q_2, \cdots, q_n)$. In the other direction, all solutions of (1.10) (without the gcd restriction) give solutions to the cyclic congruence system (1.3), but some integer solutions $(q_1, q_2, \cdots q_n)$ to the cyclic congruence system (1.3) (without the gcd restriction) may not arise this way.

The main body of this paper studies integer solutions of the Diophantine equation (1.10), and does not impose any gcd restrictions on the variables. Many special cases of this equation have been previously considered in the literature, and we discuss them below. To these results, this paper supplies necessary and sufficient conditions when these equations have infinitely many integer solutions, given in Theorem 6.1. We also establish finiteness bounds on the sizes of the solutions that apply to all other cases of the Diophantine equation (1.10), given in Theorem 3.1 and Theorem 5.1.

The existence of an infinite number of integer solutions to the equation (1.10) essentially traces back to the special case $m = 0$, which we treat in §4. We use it to obtain a characterization of which parameter values (r, s, m) allow an infinite number of solutions, which applies more generally to the affine algebraic hypersurface obtained from (1.10) by clearing denominators. This hypersurface is given by

$$r\left(\prod_{i=1}^{n}x_i\right)\left(\frac{1}{x_1}+\cdots+\frac{1}{x_n}\right)+s=m\left(\prod_{i=1}^{n}x_i\right). \tag{1.11}$$

The following theorem gives necessary and sufficient conditions on (r, s, m) for this Diophantine equation to have infinitely many integer solutions.

Theorem 1.4 *Let r, s be nonzero integers, with $r \geq 1$. Then for $n \geq 2$ the affine algebraic hypersurface*

$$r\left(\prod_{i=1}^{n}x_i\right)\left(\frac{1}{x_1}+\cdots+\frac{1}{x_n}\right)+s=m\left(\prod_{i=1}^{n}x_i\right) \tag{1.12}$$

defined over $\mathbb{Z}$ has infinitely many integer solutions $(x_1, x_2, \cdots, x_n) \in (\mathbb{Z} \smallsetminus \{0\})^n$ if and only if $r = 1$ and one of the following conditions hold: (i) $|m| \leq n-2$ and s is arbitrary; (ii) $m = n-1$ and $s = 1$; or (iii) $m = -(n-1)$ and $s = (-1)^{n-1}$.

For all parameter values (r, s, m) the equation (1.12) has infinitely many rational solutions $(x_1, \cdots, x_n) \in \mathbb{Q}^n$. Namely, if we fix variables $x_2, \cdots, x_n$ to take rational values, then the remaining variable x_1 is determined by a linear equation, so is rational. Thus the parameter restrictions of Theorem 1.4 are a consequence of requiring integrality of solutions.

Various authors have studied special cases of the Diophantine equation (1.10), often arising as a byproduct of studies on the Diophantine equation

$$\frac{1}{x_1}+\cdots+\frac{1}{x_n}=\frac{a}{b}, \tag{1.13}$$

which encodes the problem of representing $\frac{a}{b}$ as a sum of Egyptian fractions, where $0 < \frac{a}{b} \leq 1$. This work starts with J. J. Sylvester [15] in 1880. For $\frac{a}{b} = 1$ the double-exponential solution u_n is related to the problem of determining

$$F_n := \max\{q_n : \sum_{i=1}^{n} \frac{1}{q_i} = 1 \quad \text{with integers } q_i \geq 1\} \ . \tag{1.14}$$

It is well-known that the answer to (1.14) is

$$F_n = u_n - 1 \ , \tag{1.15}$$

in which $u_i = u_i(1)$ is the Sylvester sequence. In 1921 Kellogg [10] conjectured the equality (1.15), which was proved in 1922 independently by Curtis [4] and Takenouchi [16]. This bound was reproved in 1950 by Erdős [5], in the course of a more general investigation of Egyptian fractions which raised new questions, cf. Schinzel [13]. Another proof is given by Soundararajan [14]. The extremal solutions to this problem turn out to have last variable q_n expressible in terms of the preceding ones by $q_n = q_1 q_2 \cdots q_{n-1}$, which yields the Diophantine equation

$$\left(\frac{1}{q_1} + \frac{1}{q_2} + ... + \frac{1}{q_{n-1}}\right) + \frac{1}{q_1 q_2 ... q_{n-1}} = 1. \tag{1.16}$$

This corresponds to the case $(r, s, m) = (1, -1, 1)$ in (1.10). The equation (1.16) was directly studied by Brenton and Hill [3] in connection with complex surface singularities, and they determined a complete list of positive solutions for $n \leq 8$. Sylvester's sequence also appears in connection with certain extremal lattice point problems, see for example Zaks, Perles and Wills [17] and Hensley [9], who are concerned with the maximal volume of a lattice simplex in $\mathbb{R}^n$ containing exactly k lattice points. The author encountered cyclic congruences in studying variants of such lattice point problems, see Lagarias and Ziegler [11]. For recent work on a related lattice point problem see Nill [12].

An interesting open problem, that we do not consider, is that of estimating the number of solutions to the cyclic congruences (1.3) of size n, satisfying the side conditions (i), (ii) for given parameters (r, s). This includes as special cases that of counting the number of Giuga sequences of length n, and of counting the number of different Egyptian fractions of length n that add up to 1. Other unsolved problems about Giuga sequences are listed in Borwein et al. [2, Sect. 4] and in Borwein and Wong [1].

The contents of this paper are as follows. In §2 we give the relation of the cyclic congruence problem to solutions of the Diophantine equation (1.10). In §3 we consider positive solutions to (1.10) and use these to prove Theorem 1.1. Here a crucial ingredient (Proposition 3.1) slightly extends the method of Erdős [5]. In §4 we study solutions to (1.10) having $m = 0$, and determine when integer solutions occur in this case, with and without the side condition $gcd(x_1 \cdots x_n, s) = 1$, and use the results to prove Theorem 1.2. In §5 we show that when $m \neq 0$ there are only finitely many solutions of (1.10) having $\min\{|x_i|\} \geq 2$, and give a bound on their size, independent of m. We then use this result to prove Theorem 1.3. In §6 we determine for the case $r = 1$ the parameters (s, m) for which the Diophantine equation (1.10) has infinitely many solutions, and we use this to prove Theorem 1.4.

Acknowledgments. Part of this work was done during a visit to the Mathematical Sciences Research Institute, Berkeley, which is supported in part by NSF, and part at AT& T Labs-Research. The author thanks R. Girgensohn for bringing a result of Erdős to his attention, via Knuth, Graham and Patashnik [8, Exercise 4.59], and thanks E. Croot for discussions on the number of solutions. The author is indebted to the reviewer for many useful comments. This work was supported in part by NSF grant DMS-0500555.

2. Associated Diophantine equation

Solutions to cyclic congruences correspond to solutions of an associated Diophantine equation of type (1.10) with variable m, a fact observed by Borwein et al. [2] for Giuga sequences.

Lemma 2.1 *Let r, s be nonzero integers with $r > 0$ and $\gcd(r, s) = 1$. Then for each $n \geq 2$ the following conditions are equivalent.*

(1) The nonzero integers $(q_1, ..., q_n)$ with $\gcd(q_1 q_2 \cdots q_n, s) = 1$ satisfy the cyclic system of simultaneous congruences

$$r\left(\frac{\prod_{k=1}^{n} q_k}{q_i}\right) \equiv s \pmod{|q_i|}, \quad 1 \leq i \leq n . \tag{2.1}$$

(2) The nonzero integers $(q_1, ..., q_n)$ with $gcd(q_1 q_2 \cdots q_n, s) = 1$ satisfy the Diophantine equation

$$r\left(\frac{1}{q_1} + \cdots \frac{1}{q_n}\right) - \frac{s}{q_1 q_2 \cdots q_n} = m \tag{2.2}$$

for some integer m.

Proof. Suppose (1) holds, and write

$$M := r\left(\prod_{k=1}^{n} q_k\right)\left(\frac{1}{q_1} + \cdots + \frac{1}{q_n}\right) - s. \tag{2.3}$$

Each q_i divides the integer M, for it divides $\frac{r}{q_j}(\prod_{k=1}^{n} q_k)$ for each $j \neq i$, and it divides $r\left(\frac{\prod_{k=1}^{n} q_k}{q_i}\right) - s$ by (2.1). We conclude that the least common multiple $[q_1, q_2, \cdots, q_n]$ of the q_i divides M.

The cyclic congruence (2.1) and the fact $\gcd(q_1 q_2 \cdots q_n, s) = 1$ implies that $r\left(\frac{q_1 q_2 \cdots q_n}{q_i}\right)$ is invertible (mod $|q_i|$), whence $(q_j, q_i) = 1$ for all $j \neq i$. Thus the q_i are pairwise relatively prime, so $[q_1, q_2, \cdots, q_n] = q_1 q_2 \cdots q_m$. Thus we can write

$$M = m(q_1 q_2 \cdots q_n)$$

for some integer m. Dividing (2.3) by $q_1 q_2 \cdots q_m$ yields the Diophantine equation (2.2), which gives (2).

Suppose (2) holds, without imposing the gcd condition (**??**). Multiply (2.2) by $q_1 q_2 \cdots q_n$ to obtain

$$r\left(\sum_{i=1}^{n} \frac{q_1 q_2 \cdots + q_n}{q_i}\right) - s = m q_1 q_2 \cdots q_n,$$

Reducing this equation (mod$|q_i|$) yields a solution to the cyclic congruence (2.1) for q_i, which is (1), without imposing the gcd condition. Now imposing the gcd condition gives (1). ∎

Remarks. (1) This proof shows that solutions to the Diophantine equation (2.2) not satisfying the gcd condition $gcd(q_1 q_2 \cdots q_n, s) = 1$ still give solutions to the corresponding cyclic congruence (2.1), not satisfying the gcd condition. However the converse is not true, for one may take $n = 2$ and $(r, s) = (1, -20)$, and then $(q_1, q_2) = (5, 25)$ has $\gcd(q_1 q_2, s) = 5$ and satisfies the cyclic congruence system (2.1) but not the Diophantine equation (2.2).

(2) All solutions to the cyclic congruences (2.1) with $(q_1 \cdots q_n, s) = 1$ necessarily have

$$\gcd(mq_1 q_2 \cdots q_n, r) = 1.$$

To see this, consider the associated Diophantine equation (2.2) and multiply by all the q_i to obtain

$$r\left(\prod_{k=1}^{n} q_k\right)\left(\frac{1}{q_1} + \cdots + \frac{1}{q_n}\right) - s = m(\prod_{i=1}^{n} q_i).$$

Reducing this equation (mod r) yields

$$m \prod_{i=1}^{n} q_i \equiv s \pmod{r}.$$

Since s is invertible (mod m) we obtain $gcd(mq_1 q_2 \cdots q_n, r) = 1$.

(3) For the cyclic congurence (2.1), the side condition $\gcd(q_1 q_2 \cdots q_n, s) = 1$ holds if and only if all q_i are pairwise relatively prime, i.e. $\gcd(q_i, q_j) = 1$ if $i \neq j$. The "only if" direction was shown in the proof of Lemma 2.1. For the "if" direction, we prove the contrapositive. If $\gcd(q_1 q_2 \cdots q_n, s) > 1$, there exists some prime $p|s$ with $p|\gcd(q_i, s)$ for some index i. Then the i-th cyclic congruence $r\left(\frac{\prod_{k=1}^{n} q_k}{q_i}\right) \equiv s \pmod{|q_i|}$ yields

$$r\left(\prod_{k \neq i} q_k\right) \equiv 0 \pmod{p},$$

whence $\gcd(r, s) = 1$ yields $p|q_k$ for some $k \neq i$, so $p|\gcd(q_i, q_k)$, and the q_i are not pairwise relatively prime.

3. Positive integer solutions: Proof of Theorem 1.1

We treat the case of positive solutions $(q_1, ..., q_n)$ to the cyclic congruence (1.3), and prove Theorem 1.1. Lemma 2.1 reduces this to questions about positive integer solutions of the Diophantine equation

$$r\left(\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}\right) - \frac{s}{x_1 x_2 \cdots x_n} = z. \tag{3.1}$$

The following result gives bounds on the size of positive solutions to this equation, without imposing any gcd conditions on the solutions.

Theorem 3.1 *Suppose r, s are nonzero integers with $r \geq 1$ and $(r, s) = 1$. Then for fixed $n \geq 2$ the Diophantine equation (3.1) has only finitely many integer solutions $(x_1, x_2, \cdots, x_n, z) = (q_1, q_2, ..., q_n, m)$ satisfying $1 \leq q_1 \leq q_2 \leq \cdots \leq q_n$, and the side conditions*

$$rq_1 \cdots q_{n-1} > s, \quad \text{if} \quad s > 0, \tag{3.2}$$

$$q_n > |s| \quad \text{if} \quad s < 0, \tag{3.3}$$

and allowing any m. Furthermore, when these conditions hold:

(1) All solutions have $m \geq 1$ and satisfy the bounds

$$\max\{q_i\} \leq \begin{cases} u_n(r) - 2 & \text{if} \quad s > 0, \\ u_n(r) + |s| - 1 & \text{if} \quad s < 0. \end{cases} \tag{3.4}$$

Here $u_n(r)$ is determined by the recursion $u_1(r) = r + 1$ and

$$u_{n+1}(r) = r \left(\prod_{i=1}^{n} u_i(r) \right) + 1. \tag{3.5}$$

(2) If in addition $q_n > s^2$, then there holds

$$\max\{q_i\} \leq u_n(r) - s - 1. \tag{3.6}$$

Furthermore, whenever $u_n(r) > s^2$, there exist solutions for which $q_n = u_n(r) - s - 1$, so the bound (3.6) is tight for all (r, s, n) for which $u_n(r) > s^2$.

The condition $rq_1 \cdots q_{n-1} > s$ is needed in the theorem when $s > 0$ because the case $rq_1 \cdots q_{n-1} = s$ can sometimes have infinitely many positive solutions, when no gcd conditions are imposed. These occur when $\sum_{i=1}^{n-1} \frac{1}{q_i} = \frac{m}{r}$ for some positive integer m. The condition $q_n > |s|$ when $s < 0$ is needed for a similar reason.

We will use the following bound for a Kellogg-type Diophantine equation, which is an extension to all r of a result of Erdős [5, Tétel 5] for the case $r = 1$. (A sketch of Erdős's proof appears in Knuth, Graham and Patashnik [8, Exercise 4.59; cf. p. 523].)

Proposition 3.1 *Let $r \geq 1$ be an integer, and let $p_1, p_2, \cdots p_k$ be positive integers with $k \geq 1$ such that*

$$\sum_{i=1}^{k} \frac{1}{p_i} + \frac{1}{\alpha_{k+1}} = \frac{1}{r}. \tag{3.7}$$

in which α_{k+1} is a positive rational number such that

$$\alpha_{k+1} \geq \max\{p_1, p_2, \cdots, p_k\}. \tag{3.8}$$

Let $u_1(r) = r + 1$ and $u_{k+1}(r) = ru_1(r) \cdots u_k(r) + 1$. Then α_{k+1} satisfies the bounds

$$\alpha_{k+1} \leq u_{k+1}(r) - 1, \tag{3.9}$$

$$p_1 p_2 \cdots p_k(\alpha_{k+1} + 1) \leq u_1(r)u_2(r) \cdots u_k(r)u_{k+1}(r). \tag{3.10}$$

Proof. We prove the result by induction on $k \geq 1$. For the base case $k = 1$, (3.7) requires $p_1 \geq r + 1$, which then implies

$$\alpha_2 \leq r(r+1) = u_2(r) - 1,$$

since $\frac{1}{r+1} + \frac{1}{r(r+1)} = \frac{1}{r}$. The condition $\alpha_2 \geq p_1$ requires $r + 1 \leq p_1 \leq 2r$. To complete the base case we must verify that

$$p_1(\alpha_2 + 1) \leq (r+1)(r^2 + r + 1) = u_1(r)u_2(r).$$

To see this, we solve (3.7) for α_2, obtaining $\alpha_2 = \frac{p_1 r}{p_1 - r}$. Viewing this as a function of p_1 we set

$$f(p_1) := p_1(\alpha_2 + 1) = p_1(\frac{p_1 r}{p_1 - r} + 1).$$

We calculate for $p_1 > r$,

$$\frac{d^2 f}{dp_1^2} = \frac{2p_1 r}{p_1 - r} + \frac{2(p_1)^2 r}{(p_1 - r)^3} \geq 0.$$

Thus $f(p_1)$ is convex downwards on $r + 1 \leq p_1 \leq 2r$ so its maximum occurs at one of the endpoints of this interval. Now $f(2r) = 2r(2r + 1) \leq f(r + 1) = (r + 1)(r^2 + r + 1)$, for $r \geq 1$, giving the result.

For the induction step, we assume it is true for all values $k - 1$ or smaller and treat the given $k \geq 2$, which concerns

$$\frac{1}{p_1} + \cdots + \frac{1}{p_k} + \frac{1}{\alpha_{k+1}} = \frac{1}{r}. \tag{3.11}$$

Now there exists an integer $d \geq 1$ such that

$$\frac{1}{\alpha_{k+1}} = \frac{1}{r} - \left(\sum_{i=1}^{k} \frac{1}{p_i}\right) = \frac{d}{r p_1 p_2 \cdots p_k},$$

hence

$$\alpha_{k+1} = \frac{r p_1 p_2 \cdots p_k}{d} \leq r p_1 p_2 \cdots p_k. \tag{3.12}$$

The induction step is treated in three cases.

Case 1. $p_k > p_{k-1}$ and $\frac{1}{p_1} + \cdots + \frac{1}{p_{k-1}} + \frac{1}{p_k - 1} \geq \frac{1}{r}$.

In this case there exists a rational β_k with $p_k > \beta_k \geq p_k - 1 \geq p_{k-1}$ such that

$$\frac{1}{p_1} + \cdots + \frac{1}{p_{k-1}} + \frac{1}{\beta_k} = \frac{1}{r},$$

The induction hypothesis for $k - 1$ is satisfied for this equation, so we conclude,

$$\beta_k + 1 \leq u_k(r),$$

and, since $p_k \leq \beta_k + 1$,

$$p_1 p_2 \cdots p_k \leq p_1 p_2 \cdots p_{k-1}(\beta_k + 1) \leq u_1(r)u_2(r) \cdots u_k(r). \tag{3.13}$$

Combined with (3.12) this yields

$$\alpha_{k+1} \le r p_1 p_2 \cdots p_k \le r u_1(r) u_2(r) \cdots u_k(r) = u_{k+1}(r) - 1.$$

Consequently, using (3.13),

$$p_1 p_2 \cdots p_k (\alpha_{k+1} + 1) \le u_1(r) u_2(r) \cdots u_k(r) u_{k+1}(r),$$

completing the induction step in Case 1.

Case 2. $p_k = p_{k-1}$ and $\frac{1}{p_1} + \cdots + \frac{1}{p_{k-1}} + \frac{1}{p_k - 1} \ge \frac{1}{r}$.

We may suppose $p_k \ge 4$, for the only case with $p_k \le 3$ has $p_k = p_{k-1} = 3$ with $k = 2, r = 1$ and $\alpha_{k+1} = 3$, which satisfies the theorem. When $p_k \ge 4$ we have $\frac{1}{p_k - 2} \le \frac{2}{p_k} = \frac{1}{p_k} + \frac{1}{p_{k-1}}$, so there exists $\beta_k > 0$ such that

$$\frac{1}{p_1} + \cdots + \frac{1}{p_{k-2}} + \left(\frac{1}{p_k - 2} + \frac{1}{\beta_k} \right) = \frac{1}{r}. \tag{3.14}$$

We claim that

$$(p_k)^2 \le (p_k - 2)(\beta_k + 1). \tag{3.15}$$

Assuming this claim is proved, it implies $\beta_k > p_k$, hence the equation (3.14) satisfies the induction hypothesis for $k - 1$. This yields

$$p_1 p_2 \cdots p_{k-2} p_{k-1} p_k \le p_1 p_2 \cdots p_{k-2} (p_k - 2)(\beta_k + 1) \le u_1(r) u_2(r) \cdots u_k(r).$$

Then using (3.12) we obtain

$$\alpha_{k+1} \le r p_1 p_2 \cdots p_k \le r u_1(r) u_2(r) \cdots u_k(r) = u_{k+1}(r) - 1.$$

Consequently

$$p_1 p_2 \cdots p_k (\alpha_{k+1} + 1) \le u_1(r) u_2(r) \cdots u_k(r) u_{k+1}(r),$$

completing the induction step in case 2.

It remains to prove the claim (3.15). Subtracting (3.11) from (3.14) and using $p_k = p_{k-1}$ gives

$$\frac{1}{\beta_k} = \frac{1}{\alpha_{k+1}} + \left(\frac{2}{p_k} - \frac{1}{p_k - 2} \right).$$

The Case 2 hypothesis gives

$$\frac{1}{\alpha_{k+1}} \le \frac{1}{p_k - 1} - \frac{1}{p_k} = \frac{1}{p_k (p_k - 1)},$$

so that

$$\frac{1}{\beta_k} \le \frac{1}{p_k (p_k - 1)} + \frac{2}{p_k} - \frac{1}{p_k - 2} = \frac{(p_k)^2 - 4p_k + 2}{p_k (p_k - 1)(p_k - 2)}.$$

Setting $y = p_k$, this yields

$$\beta_k \ge \frac{y(y-1)(y-2)}{y^2 - 4y + 2}.$$

from which we obtain

$$(p_k - 2)(\beta_k + 1) \geq \frac{y(y-1)(y-2)^2}{y^2 - 4y + 2}.$$

Now (3.15) follows from the inequality

$$\frac{y(y-1)(y-2)^2}{y^2 - 4y + 2} \geq y^2 \quad \text{for} \quad y \geq 4,$$

which is easily verified by clearing the denominator and simplifying.

Case 3. $\frac{1}{p_1} + \cdots + \frac{1}{p_{k-1}} + \frac{1}{p_k - 1} < \frac{1}{r}$.

For reasons as in case 2, we may suppose $p_k \geq 5$. In this case we replace p_k by $\tilde{p}_k := p_k - 1$, and α_{k+1} by $\tilde{\alpha}_{k+1}$ satisfying

$$\frac{1}{p_k} + \frac{1}{\alpha_{k+1}} = \frac{1}{p_k - 1} + \frac{1}{\tilde{\alpha}_{k+1}}, \tag{3.16}$$

The case 3 inequality guarantees that $\tilde{\alpha}_{k+1}$ is positive, which ensures that $\tilde{\alpha}_{k+1} > \alpha_{k+1} \geq p_k$. We claim that in addition

$$p_k(\alpha_{k+1} + 1) \leq (p_k - 1)(\tilde{\alpha}_{k+1} + 1). \tag{3.17}$$

Assuming this claim is proved, we have obtained a new equation of the same size k,

$$\frac{1}{p_1} + \cdots + \frac{1}{p_{k-1}} + \left(\frac{1}{p_k - 1} + \frac{1}{\tilde{\alpha}_{k+1}}\right) = \frac{1}{r},$$

which has new denominators $(p_1, ..., p_{k-2}, p_{k-1}, \tilde{p}_k)$, which are the same or smaller than the original system, while $\tilde{\alpha}_{k+1}$ has increased. It then suffices to prove the induction step for the new equation because it would give

$$\alpha_{k+1} \leq \tilde{\alpha}_{k+1} \leq u_{k+1}(r) - 1$$

$$p_1 \cdots p_{k-1} p_k(\alpha_{k+1} + 1) \leq p_1 \cdots p_{k-1}(p_k - 1)(\tilde{\alpha}_{k+1} + 1) \leq u_1(r)u_2(r) \cdots u_k(r)u_{k+1}(r),$$

thus proving the induction step for the original equation. If the new system falls in case 1 or 2 we are done, while if it falls in case 3 we can repeat the reduction. Eventual termination into case 1 or 2 must occur, because the sum of the denominators decreases at each step. Thus case 3 will terminate.

It remains to prove the claim (3.17). Using the definition (3.16) of $\tilde{\alpha}_{k+1}$, we express it in terms of $y = p_k$ and α_{k+1}, obtaining

$$\tilde{\alpha}_{k+1} = \frac{y(y-1)\alpha_{k+1}}{y(y-1) - \alpha_{k+1}},$$

noting that $y(y-1) > \alpha_{k+1}$ under the Case 3 hypothesis. Substituting this in the inequality (3.17) and clearing a positive denominator shows that it is equivalent to

$$(\frac{y}{y-1})\alpha_{k+1}^2 - (y+1)\alpha_{k+1} + y(y-1) \geq 0,$$

when $\alpha_{k+1} \geq y \geq 5$. The left side is a quadratic polynomial in α_{k+1} having discriminant $D = (y+1)^2 - 4y^2$, and $D < 0$ when $y > 1$, hence it is then positive for all real α_{k+1} and the inequality (3.17) follows. This completes Case 3. ∎

We use Proposition 3.1 to establish Theorem 3.1.

Proof of Theorem 3.1. We first eliminate all values $q_i = 1$, which reduces the equation (3.1) to an equation in fewer x-variables having the same form, with z shifted by an integer, and without affecting the side conditions. The bound to be proved is nondecreasing in n and independent of z, so it suffices to prove the upper bound for the new system, which has solutions satisfying $2 \leq q_1 \leq q_2 \leq \cdots \leq q_n$. We denote the associated integer choice of the z variable by m. Now we can rewrite a solution to (3.1) as

$$\sum_{i=1}^{n} \frac{1}{p_i} + \frac{1}{\alpha_{n+1}} = \frac{m}{r}, \tag{3.18}$$

where we have $p_i := q_i$ and $\alpha_{n+1} := -\frac{r}{s} q_1 q_2 \cdots q_n$, where α_{n+1} may be positive or negative, depending on the sign of s.

Case 1. $s > 0$.

We claim that $rq_1 \cdots q_{n-1} > s$ implies $m \geq 1$. To show this, note that we always have, for some integer $b > 0$,

$$\left(\sum_{i=1}^{n-1} \frac{1}{q_i}\right) + \frac{1}{q_n}\left(1 - \frac{s}{rq_1 q_2 \cdots q_{n-1}}\right) = \frac{b}{q_1 \cdots q_{n-1}} + \frac{1}{q_n}\left(1 - \frac{s}{rq_1 q_2 \cdots q_{n-1}}\right) = \frac{m}{r}. \tag{3.19}$$

The condition $rq_1 q_2 \cdots q_{n-1} > s$ implies that the coefficient of $\frac{1}{q_n}$ is positive, so we may legitimately solve this equation for q_n, obtaining

$$q_n = \frac{1 - \frac{s}{rq_1 q_2 \cdots q_{n-1}}}{\frac{m}{r} - \frac{b}{q_1 q_2 \cdots q_{n-1}}} = \frac{rq_1 q_2 \cdots q_{n-1} - s}{mq_1 \cdots q_{n-1} - rb}. \tag{3.20}$$

Here the denominator of the fraction cannot vanish, since $q_n < \infty$. If now $m \leq 0$, then the denominator of the fraction on the right in (3.20) would be negative, while the numerator is positive, contradicting $q_n > 0$. Thus $m \geq 1$, and the claim is proved.

Now we divide (3.19) by $m \geq 1$ to obtain

$$\left(\sum_{i=1}^{n-1} \frac{1}{mq_i}\right) + \left(\frac{1}{mq_n} - \frac{s}{mrq_1 q_2 \cdots q_n}\right) = \frac{1}{r}. \tag{3.21}$$

We view this as an instance of Proposition 3.1, with $k = n-1$, setting $p_i = mq_i$ for $1 \leq i \leq n-1$, and

$$\frac{1}{\alpha_n} := \frac{1}{mq_n} - \frac{s}{mrq_1 q_2 \cdots q_n} = \frac{1}{mq_n}\left(1 - \frac{s}{rq_1 q_2 \cdots q_{n-1}}\right).$$

Now we have

$$\alpha_n = mq_n \left(\frac{rq_1q_2\cdots q_{n-1}}{rq_1q_2\cdots q_{n-1} - s} \right), \tag{3.22}$$

and $rq_1\cdots q_{n-1} > s$ yields

$$\alpha_n > mq_n \geq mq_{n-1} = p_{n-1} > 0, \tag{3.23}$$

so the hypotheses of Proposition 3.1 are satisfied for (3.21). The proposition then gives

$$\alpha_n \leq u_n(r) - 1, \tag{3.24}$$

$$q_1q_2\cdots q_{n-1}(\alpha_n + 1) \leq u_1(r)u_2(r)\cdots u_n(r). \tag{3.25}$$

Solving (3.22) for q_n yields

$$q_n = \frac{1}{m}\left(1 - \frac{s}{rq_1q_2\cdots q_{n-1}}\right)\alpha_n \leq \frac{1}{m}\left(1 - \frac{1}{rq_1q_2\cdots q_{n-1}}\right)(u_n(r) - 1).$$

Now (3.25) implies

$$\begin{aligned} \frac{s}{rq_1\cdots q_{n-1}} &= \frac{s(\alpha_n+1)}{rq_1\cdots q_{n-1}(\alpha_n+1)} \\ &\geq \frac{s(\alpha_n+1)}{ru_1(r)\cdots u_{n-1}(r)u_n(r)} = \frac{s(\alpha_n+1)}{(u_n(r)-1)u_n(r)}. \end{aligned}$$

From (3.22) and (3.23) we then deduce

$$\begin{aligned} q_n &\leq u_n(r) - 1 - \frac{s(\alpha_n+1)}{u_n(r)} \\ &\leq u_n(r) - 1 - \frac{s(mq_n)}{u_n(r)} \\ &\leq u_n(r) - 1 - \lceil \frac{sq_n}{u_n(r)} \rceil. \end{aligned} \tag{3.26}$$

From this inequality we immediately deduce that for $q_n > 1$,

$$q_n \leq u_n(r) - 2. \tag{3.27}$$

We also deduce that, for $q_n > s^2$, there holds

$$q_n \leq u_n(r) - s - 1. \tag{3.28}$$

Suppose otherwise, so that $q_n \geq u_n(r) - s$. Then (3.26) gives,

$$u_n(r) - s \leq q_n \leq u_n(r) - 1 - \lceil s - \frac{s^2}{u_n(r)} \rceil = u_n(r) - s - 1 + \lfloor \frac{s^2}{u_n(r)} \rfloor = u_n(r) - s - 1,$$

a contradiction which establishes (3.28).

Case 2. $s < 0$.
Now the left side of (3.1) has every term positive, which implies that $z = m > 0$, so again $m \geq 1$. Dividing by m we obtain

$$\left(\sum_{i=1}^{n-1} \frac{1}{mq_i}\right) + \frac{1}{mq_n} + \frac{|s|}{mrq_1 \cdots q_n} = \frac{1}{r}. \tag{3.29}$$

By hypothesis $q_n > |s|$, and we consider a new system that replaces q_n by $q_n - |s|$. Now there is an integer b such that

$$\left(\sum_{i=1}^{n-1} \frac{1}{mq_i}\right) + \frac{1}{m(q_n - |s|)} + \frac{b}{mrq_1 \cdots q_{n-1}(q_n - |s|)} = \frac{1}{r}. \tag{3.30}$$

Subtracting (3.29) from this equation and rearranging terms yields

$$\begin{aligned} \frac{b}{mrq_1 \cdots q_{n-1}(q_n - |s|)} &= \frac{1}{mq_n} + \frac{|s|}{mrq_1 \cdots q_n} - \frac{1}{m(q_n - |s|)} \\ &= \frac{rq_1 \cdots q_{n-1}(q_n - |s|) + |s|(q_n - |s|) - rq_1 \cdots q_n}{mrq_1 \cdots q_{n-1}q_n(q_n - |s|)} \\ &= \frac{|s|(q_n - |s| - rq_1 \cdots q_{n-1})}{mrq_1 \cdots q_{n-1}q_n(q_n - |s|)} \end{aligned}$$

Comparing both sides yields

$$b = |s| \left(1 - \frac{rq_1q_2 \cdots q_{n-1} + |s|}{q_n}\right). \tag{3.31}$$

We claim $b \leq 0$, which is the same as

$$q_n \leq rq_1q_2 \cdots q_{n-1} + |s|. \tag{3.32}$$

To show this, note that there is a positive integer b' such that

$$\frac{1}{r} - \left(\sum_{i=1}^{n-1} \frac{1}{mq_i}\right) = \frac{b'}{mrq_1 \cdots q_{n-1}} \geq \frac{1}{mrq_1 \cdots q_{n-1}}. \tag{3.33}$$

By (3.29) the left side of this expression equals

$$\frac{1}{mq_n}(1 + \frac{|s|}{rq_1 \cdots q_{n-1}}) = \left(\frac{rq_1 \cdots q_{n-1} + |s|}{mq_n}\right) \frac{1}{mrq_1 \cdots q_{n-1}}.$$

Comparison with (3.33) yields (3.32), proving the claim.

We treat two subcases, $b = 0$ and $b < 0$.

Subcase 2.1. $b = 0$.

In this subcase we have

$$\left(\sum_{i=1}^{n-1} \frac{1}{mq_i}\right) + \frac{1}{m(q_n - |s|)} = \frac{1}{r}.$$

This is a system of the form of Proposition 3.1 for $k = n-1$, after permuting the terms to take $\alpha_n = \max\{mq_i, m(q_n - |s|)\}$. We conclude from the proposition that

$$q_n - |s| \leq m(q_n - |s|) \leq \alpha_n \leq u_n(r) - 1.$$

Then we deduce

$$q_n \leq (q_n - |s|) + |s| \leq u_n(r) + |s| - 1.$$

Subcase 2.2. $b < 0$.

In this subcase we have

$$\left(\sum_{i=1}^{n-1} \frac{1}{mq_i}\right) + \frac{1}{m(q_n - |s|)} - \frac{|b|}{mrq_1q_2\cdots q_{n-1}(q_n - |s|)} = \frac{1}{r},$$

which is a system of the form (3.1) with new variables $(q_1', \cdots, q_n') := (q_1, \cdots, q_{n-1}, q_n - |s|)$ and $z = m$, and with new parameters $(r', s') = (r, |b|)$. We claim this system falls under Case 1, taking $s' = |b| > 0$, possibly after permuting the variables. We must verify that two side conditions hold, namely $q_n' = q_n - |s| > 0$ and

$$rq_1'q_2'\cdots q_{n-1}' > |b|. \tag{3.34}$$

The first of these holds by hypothesis. For the second, we observe that (3.34) is equivalent to

$$rq_1q_2\cdots q_{n-1} + |s| > |b| + |s|. \tag{3.35}$$

But now (3.31) gives (since both $b, s < 0$),

$$|b| + |s| = \frac{|s|(rq_1q_2\cdots q_{n-1} + |s|)}{q_n} = (rq_1q_2\cdots q_{n-1} + |s|)\frac{|s|}{q_n} < rq_1q_2\cdots q_{n-1} + |s|,$$

which verifies (3.35). Thus the Case 1 hypotheses are met for the new system.

We now apply the Case 1 inequality in the form (3.27) to obtain

$$q_n - |s| \leq \max\{q_i'\} \leq u_n(r) - 2,$$

and this yields

$$q_n \leq u_n(r) + |s| - 2,$$

in Subcase 2.2.

Combining the two subcases, we conclude that in Case 2 one always has

$$q_n \leq u_n(r) + |s| - 1 = u_n(r) - s - 1,$$

as required.

To finish the proof it remains to verify the tightness of the upper bounds $u_n(r) - s - 1$ for given nonzero r, s with $r > 0$ and $gcd(r, s) = 1$, for those n having solutions with $q_n > s^2$ if $s > 0$ and $q_n > |s|$ if $s < 0$. We show the existence of solutions with $q_n = u_n - s - 1$. One verifies, by induction on n, that

$$(x_1, x_2, \cdots, x_n) = (u_1(r), u_2(r), \cdots, u_{n-1}(r), u_n(r) - s + 1)$$

gives a solution to (3.1) with $z = 1$ for all pairs (r, s) whenever $u_n(r) - s + 1 \geq 2$. The key property is that

$$\frac{1}{r} - \left(\sum_{i=1}^{n-1} \frac{1}{u_i(r)} \right) = \frac{1}{r u_1(r) u_2(r) \cdots u_n(r)},$$

and

$$-\frac{1}{r u_1(r) u_2(r) \cdots u_{n-1}(r)} + \frac{1}{r u_1(r) \cdots u_{n-1}(r) - s} = \frac{s}{r u_1(r) \cdots u_{n-1}(r)(u_n(r) - s - 1)}.$$

Note also that $gcd(q_1 q_2 \cdots q_n, r) = 1$ always holds for these solutions, using $gcd(r, s) = 1$, but $\gcd(q_1 q_2 \cdots q_n, s) > 1$ may occur for certain $|s| > 1$. ∎

We now deduce Theorem 1.1 from Theorem 3.1.

Proof of Theorem 1.1. To bound the size of a positive solution $(q_1, ..., q_n)$ to the cyclic congruence, we first drop all variables $q_i = 1$, which reduces to a cyclic congruence in fewer variables, but necessarily at least two variables, since at least two $q_i \geq 2$. The desired upper bounds (1.6) are all nondecreasing functions of n so it suffices to treat the smaller problem. Thus we may assume all $q_i \geq 2$, and we may reorder the variables so that $2 \leq q_1 \leq q_2 \leq \cdots \leq q_n$, with $n \geq 2$.

We then use Lemma 2.1 to convert the cyclic congruence solution $(q_1, ..., q_n)$ to a solution of a Diophantine equation (3.1) with some value of z, and we may presume this solution is large enough to satisfy the side conditions (3.2) and (3.3) in Theorem 3.1. The equation we consider is then

$$\left(\sum_{i=1}^{n} \frac{1}{q_i} \right) - \frac{s}{r q_1 q_2 \cdots q_n} = \frac{m}{r}. \tag{3.36}$$

By the discussion after Lemma 2.1 the hypotheses $\gcd(q_1 \cdots q_n, s) = 1$ implies $\gcd(q_i, q_j) = 1$ if $i \neq j$ and $\gcd(m q_1 \cdots q_n, r) = 1$. Thus we must have $2 \leq q_2 < q_3 < \cdots < q_n$.

We show finiteness of the number of solutions. Consider first the case $s < 0$. Theorem 3.1 establishes finiteness of solutions having $q_n > s$. Finiteness of solutions having $q_n \leq s$ is immediate, since they then satisfy $2 \leq q_1 < q_2 < \cdots < q_n \leq s$. Now consider the remaining cases $s > 0$. Theorem 3.1 also establishes finiteness of the number of solutions, for fixed $s > 0$, that satisfy $r q_1 \cdots q_{n-1} > s$. For the remaining cases with $r q_1 \cdots q_{n-1} \leq s$, we establish finiteness of the admissible solutions (those having $\gcd(q_1 \cdots q_n, s) = 1$) by obtaining an upper bound for q_n, namely $q_n < s$. We first show there are no admisible solutions in the equality case $r q_1 q_2 \cdots q_{n-1} = s$. For $|s| \geq 2$ this holds since $(q_1 \cdots q_n, s) = 1$ and $(r, s) = 1$ by hypothesis, and for $s = \pm 1$ it holds because $q_1 \geq 2$. (The equality case is a critical case, for a single solution to

it would yield infinitely many positive solutions to (1.4), since q_n is unconstrained.) It remains to treat cases where $rq_1 \cdots q_n < s$. Now we have, by (3.20), that the Diophantine equation can be solved for q_n,

$$q_n := \frac{rq_1q_2 \cdots q_{n-1} - s}{mq_1 \cdots q_{n-1} - rb}, \tag{3.37}$$

where

$$\sum_{i=1}^{n-1} \frac{1}{mq_i} = \frac{b}{mrq_1 \cdots q_{n-1}}.$$

The numerator in (3.37) does not vanish, and the finiteness of q_n requires the denominator be nonzero, whence

$$q_n \le |rq_1q_2 \cdots q_{n-1} - s| = s - rq_1 \cdots q_n < s.$$

Thus finiteness follows.

The explicit bounds follow from Theorem 3.1 . The condition $u_{n-1}(r) > s$ implies that $ru_1(r) \cdots u_{n-1}(r) > s$ and that

$$u_n(r) = (u_{n-1}(r) - 1)u_{n-1}(r) \ge s(s+1) > s^2,$$

so the desired conclusion $q_n \le u_n(r) - s + 1$ follows in these cases. ∎

4. General integer solutions with $m = 0$: Proof of Theorem 1.2

In the remainder of the paper we study general integer solutions $(x_1, \cdots, x_n)$ to the Diophantine equation

$$r\left(\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}\right) - \frac{s}{x_1x_2 \cdots x_n} = m, \tag{4.1}$$

in which r, s are integers with $r > 0$ and $\gcd(r, s) = 1$. In this section we treat the special case $m = 0$. We show that infinitely many solutions occur when $r = 1$, and then characterize when an infinite number of solutions exist satisfying extra gcd conditions. We apply these results to prove Theorem 1.2.

Theorem 4.1 *Suppose r, s are nonzero integers with $r > 0$ and $\gcd(r, s) = 1$. Consider the Diophantine equation*

$$r\left(\sum_{i=1}^{n} \frac{1}{x_i}\right) = \frac{s}{x_1x_2 \cdots x_n} \tag{4.2}$$

Then:

(1) If $r > 1$ this equation has no integer solutions $(x_1, \cdots, x_n)$.

(2) If $r = 1$ this equation has infinitely many integer solutions. Moreover there are infinitely many integer solutions having $\min\{|x_i|\} \ge 2$.

Proof. (1) Suppose $r \geq 2$ and that an integer solution $(x_1, \cdots, x_n)$ exists. Then

$$\sum_{i=1}^{n} \frac{1}{x_i} = \frac{s}{r x_1 \cdots x_n}.$$

However

$$\sum_{i=1}^{n} \frac{1}{x_i} = \frac{b}{x_1 x_2 \cdots x_n} = \frac{br}{x_1 x_2 \cdots x_n},$$

for some integer b. Thus $s = br$, which contradicts $\gcd(r, s) = 1$ since $r \geq 2$.

(2) Now let $r = 1$. Define the sequence $\{v_k(m) : k \geq 0\}$ for each $m \geq 1$ by the recurrence $v_1(m) = m$ and

$$v_k(m) := (v_1(m)v_2(m) \cdots v_{k-1}(m)) + 1, \tag{4.3}$$

which gives the sequence $(m, m+1, m(m+1)+1, \cdots)$. One proves, by induction on $n \geq 2$, that

$$-\frac{1}{v_1(m)} + \left(\sum_{i=2}^{n-1} \frac{1}{v_i(m)} \right) = \frac{-1}{v_1(m)v_2(m) \cdots v_{n-1}(m)}. \tag{4.4}$$

Now we obtain

$$\begin{aligned} -\frac{1}{v_1(m)} + \left(\sum_{i=2}^{n-1} \frac{1}{v_i(m)} \right) + \frac{1}{v_n(m) + (s-1)} &= -\frac{1}{v_1(m) \cdots v_{n-1}(m)} + \frac{v_1(m) \cdots v_{n-1}(m) + s}{} \\ &= \frac{-s}{v_1(m) \cdots v_{n-1}(m)(v_n(m) - s)}. \end{aligned} \tag{4.5}$$

It follows that, for $m > |s| + 1 \geq 2$,

$$(x_1, \cdots, x_{n-1}, x_n) := (-v_1(m), v_2(m), \cdots, v_{n-1}(m), v(n)(m) - s)$$

satisfies

$$\sum_{i=1}^{n} \frac{1}{x_i} = \frac{s}{x_1 \cdots x_n}$$

since $x_1 = x_1(m) < 0$ and all other $x_i = x_i(m) > 0$, and $\min\{|x_i|\} \geq 2$. ∎

The next result shows that if we require that infinitely many integer solutions satisfying the extra condition $gcd(x_1 x_2 \cdots x_n, s) = 1$ required in the cyclic congruence, then the set of parameters allowing such solutions narrows slightly. By Theorem 4.1 we need only consider the case that $r = 1$. In part (1) of the following result we include integer solutions in which some variables $x_i = \pm 1$.

Theorem 4.2 *Let s be a nonzero integer, and consider the Diophantine equation*

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} = \frac{s}{x_1 x_2 \cdots x_n}, \tag{4.6}$$

where $n \geq 2$.

(1) This equation has infinitely many integer solutions $(x_1, ..., x_n)$ with at least two $|x_i| \geq 2$ and $\gcd(x_1 x_2 \cdots x_n, s) = 1$ for those (n, s) such that $\gcd(s, M_n) = 1$, where $M_{2k} = 1$ and

$M_{2k+1} = 2$. *For all remaining* (n, s), *where* n *is odd and* s *is even, this equation has no integer solutions.*

(2) For each $n \geq 2$ *there is a finite modulus* M_n^* *such that whenever* $\gcd(s, M_n^*) = 1$ *this equation has infinitely many integer solutions satisfying* $\min\{|x_i|\} \geq 2$ *with* $\gcd(x_1 x_2, \cdots x_n, s) = 1$. *One can take* $M_n^* = u_1 u_2 \cdots u_n$, *where the* u_i *belong to Sylvester's sequence.*

Proof. (1) *Necessity.* We show there are no solutions with $\gcd(x_1 x_2 \cdots x_n, s) = 1$ when $n \equiv 1 \pmod 2$ and s is even. The gcd condition implies that all x_i are odd, and multiplying (4.6) by $x_1 x_2 \cdots x_n$ yields

$$\sum_{i=1}^{n} \frac{x_1 x_2 \cdots x_n}{x_1} = s. \tag{4.7}$$

Now the left side is odd, being a sum of n odd terms, and the right side is even, a contradiction.

Sufficiency. Suppose $n \geq 5$. Choosing $x_n = 1, x_{n-1} = 1$ leads to an equation of the same form with $n-2$ variables, and with s replaced by $-s$. In this way we reduce to the cases $n = 2$ with any s and to $n = 3$ with an odd s, and it remains to show infinitely many solutions having $\gcd(x_1 \cdots x_n, s) = 1$ exist in these cases. For $n = 2$ we have the infinite family of solutions $(x_1, x_2) = (-m, m + s)$ giving

$$-\frac{1}{m} + \frac{1}{m+s} = \frac{s}{(-m)(m+s)},$$

taking $m \geq |s| + 2$. It now suffices to restrict to the arithmetic progression $m \equiv 1 \pmod{|s|}$. For $n = 3$ we consider the family $(x_1, x_2, x_3) = (-m, m+1, m(m+1)+s)$, for $m \geq |s| + 2$. Here s is odd, so if we again choose $m \equiv 1 \pmod{|s|}$, then $(-m(m+1)(m+s), s) = 1$.

(2) Theorem 4.1 exhibited for each n and each fixed $s \neq 0$ an infinite family of solutions to (4.7) having $\min\{|x_i(m)|\} \geq 2$. Now the sequence $m \equiv 1 \pmod s$ will have the required property $gcd(x_(m) \cdots x_n(m), s) = 1$, as long as $(x_1(1) \cdots x_n(1), s) = 1$, since the congruence $x_j(1 + ks) \equiv x_j(1) \pmod{|s|}$ is easy to establish. Now we have $x_j(1) \equiv v_j(1) = u_j \pmod s$, whence

$$x_1(1) \cdots x_n(1) = (v_1(1) v_2(1) \cdots v_{n-1}(1)(v_n(1) - s) \equiv u_1 u_2 \cdots u_n (\text{mod } s).$$

Thus if we take $M_n^* = u_1 u_2 \cdots u_n$, then $\gcd(M_n^*, s) = 1$ will imply $(q_1(1+jm) \cdots q_n(1+jm), s) = 1$, for all j. ∎

Remark. One might conjecture that the minimal allowable value of M_n^* in Theorem 4.2 equals $M_n = gcd(n+1, 2)$. The necessity part of the proof above showed that one can take $M_2^* = M_2 = 1$ and $M_3^* = M_3 = 2$, confirming this conjecture in these cases.

Proof of Theorem 1.2. (1) For $r = 1$, the cyclic congruence (1.4) becomes (1.7). We show for each n and all nonzero s the latter cyclic congruence has infinitely many nontrivial solutions satisfying the gcd condition. Theorem 4.2 (1), together with Lemma 2.1, shows on choosing $m = 0$ that there are infinitely many nontrivial solutions to (1.4) when $r = 1$ and $\gcd(s, M_n) = 1$, having $\min\{|q_i|\} \geq 2$. This handles all s when n is even. If n is odd, we choose one variable

$q_n = 1$. Eliminating this variable, whose cyclic congruence (mod q_n) is trivially satisfied, yields a cyclic congruence in $(n-1)$ variables with the same $(r,s) = (1,s)$, which now has infinitely many nontrivial solutions satisfying $\gcd(q_1 \cdots q_{n-1}, s) = 1$ by Theorem 4.2(1) since $n-1$ is even.

(2) This follows similarly from Theorem 4.2 (2) together with Lemma 2.1. ∎

5. General integer solutions: Proof of Theorem 1.3

In this section we prove a finiteness theorem on the number of integer solutions to (1.10) with $m \neq 0$, with all variables $|x_i| \geq 2$, but with no gcd condition on solutions, and apply this result to prove Theorem 1.3.

Theorem 5.1 *Let r, s be integers with $r > 0$ and $\gcd(r,s) = 1$. Suppose $m \neq 0$ is fixed. Then the Diophantine equation*

$$r\left(\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}\right) - \frac{s}{x_1 x_2 \cdots x_n} = m \tag{5.1}$$

has finitely many integer solutions satisfying

$$\min\{|x_i|\} \geq 2.$$

All such solutions satisfy the bound

$$\max\{|x_i|\} \leq r^{2^{n-1}} \left(\prod_{j=1}^{n-1} (n+2-j)^{2^{n-1-j}} \right) + |s|. \tag{5.2}$$

Proof. We first note that the hypotheses imply $\gcd(mx_1 \cdots x_n, r) = 1$. This follows by multiplying by $x_1 \cdots x_n$ and then reducing (mod r), obtaining

$$mx_1 x_2 \cdots x_n \equiv -s \pmod{r},$$

and the gcd result follows since $\gcd(r,s) = 1$.

Without loss of generality reorder the variables so that $2 \leq |x_1| \leq |x_2 \leq \cdots \leq |x_n|$. We rewrite (5.1) as

$$\frac{1}{x_1} + \cdots + \frac{1}{x_n} - \frac{s}{r x_1 \cdots x_n} = \frac{m}{r}. \tag{5.3}$$

Now set

$$R_i := \left(\frac{1}{x_i} + \frac{1}{x_{i+1}} + \cdots + \frac{1}{x_n}\right) - \frac{s}{r x_1 \cdots x_n} \tag{5.4}$$

Now (5.3) gives

$$|R_1| = \frac{|m|}{r} > 0.$$

Assuming that $|x_n| > |s|$ we have

$$|R_1| \leq \frac{1}{|x_1|}\left(n + \frac{|s|}{r|x_2 \cdots x_n|}\right) \leq \frac{1}{|x_1|}(n+1).$$

This implies

$$|x_1| \le \frac{1}{R_1}(n+1) \le \frac{r}{|m|}(n+1) \le r(n+1). \tag{5.5}$$

Now (5.3) yields

$$R_i = \frac{m}{r} - \left(\frac{1}{x_1} + \cdots + \frac{1}{x_{i-1}}\right) = \frac{m_i}{r x_1 x_2 \cdots x_{i-1}} \tag{5.6}$$

with

$$m_i := m x_1 x_2 \cdots x_{i-1} - r x_1 x_2 \cdots x_{i-1} \left(\sum_{j=1}^{i-1} \frac{1}{x_j}\right). \tag{5.7}$$

We claim that $m_i \neq 0$. This follows since

$$m_i \equiv m x_1 x_2 \cdots x_{i-1} \pmod{r},$$

and we have shown $(m x_1 \cdots x_n, r) = 1$. Thus we obtain

$$|R_i| \ge \frac{1}{r|x_1 \cdots x_{i-1}|}. \tag{5.8}$$

Combining this with the definition (5.4) yields

$$\frac{1}{r|x_1 \cdots x_{i-1}|} \le |R_i| \le \frac{1}{|x_i|}\left(n - i + 1 + \frac{|s x_i|}{r|x_1 \cdots x_n|}\right)$$

and this gives, for $2 \le i \le n-1$

$$|x_i| \le r|x_1 \cdots x_{i-1}|(n-i+2) \le \tag{5.9}$$

To bound the last variable we use

$$R_n = \frac{m_n}{r x_1 \cdots x_{n-1}} = \frac{1}{x_n}\left(1 - \frac{s}{r x_1 \cdots x_{n-1}}\right)$$

which can be solved for x_n to give

$$x_n = \frac{r x_1 \cdots x_{n-1} - s}{m_n}.$$

Since $m_n \neq 0$, this yields

$$|x_n| \le r|x_1 x_2 \cdots x_{n-1}| + |s|. \tag{5.10}$$

Now (5.9) yields, by induction on $i \ge 1$, for $1 \le i \le n-1$,

$$|x_i| \le r^{2^{i-1}} \left(\prod_{j=1}^{i-1} (n+2-j)^{2^{i-1-j}}\right)(n+2-i)$$

with the base case given by (5.5). Finally, (5.10) now gives

$$|x_n| \le r^{2^{n-1}} \left(\prod_{j=1}^{n-1} (n+2-j)^{2^{n-1-j}}\right) + |s|,$$

completing the proof. ∎.

We now deduce Theorem 1.3 from this result.

Proof of Theorem 1.3. We have $r \geq 2$. By Lemma 2.1 this corresponds to a Diophantine equation of the type (5.1) with some value of m. We eliminate variables $x_i = \pm 1$, reducing to a similar system with smaller n, and with a new $s' = \pm s$, and a new value m'. If the reduced system has $n = 0$, then all $|x_i| = 1$. If the reduced system has $n = 1$, i.e. all but one variable have $|x_i| = 1$, say for $i \geq 2$, we obtain the reduced system

$$\frac{r}{x_1} - \frac{s}{x_1} = m.$$

Since $r \geq 2$ and $\gcd(r, s) = 1$ we have $r - s \neq 0$, and the only choices of x_1 giving integer m have $|x_1|$ dividing $|r - s|$, so $|x_1| \leq r + |s|$, and (1.9) holds. Finally, if the reduced system has $n \geq 2$ then this system cannot have $m' = 0$, because Theorem 4.1(1) says there are no solutions to the resulting Diophantine equation with $m = 0$. Thus $m \neq 0$, and the bound of Theorem 5.1 applies. This bound (5.2) is stronger than what is needed, since

$$r^{2^{n-1}} \left(\prod_{j=1}^{n-1} (n+2-j)^{2^{n-1-j}} \right) + |s| \leq \left(r(n+1)\right)^{2^{n-1}} + |s|,$$

which gives (1.9). ∎

6. General integer solutions: Proof of Theorem 1.4

We now determine for arbitrary m and $\gcd(r, s) = 1$ when the Diophantine equation (5.1) has infinitely many integer solutions, and apply this result to prove Theorem 1.4. The following result classfies when an infinite number of solutions exists for $r = 1$.

Theorem 6.1 *Suppose that $r = 1$, and s is nonzero. Then the Diophantine equation*

$$\left(\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} \right) - \frac{s}{x_1 x_2 \cdots x_n} = m \tag{6.1}$$

has infinitely many integer solutions if and only if (i) $|m| \leq n - 2$ and s is arbitrary, or (ii) $m = n - 1$ and $s = 1$, or (iii) $m = -(n - 1)$ and $s = (-1)^{n-1}$.

Proof. *Necessity.* We may suppose $1 \leq |x_1| \leq |x_2| \leq \cdots \leq |x_n|$. We first show there are finitely many solutions when $|m| \geq n$. Set

$$R := \frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} \tag{6.2}$$

so that (6.1) becomes

$$R + \frac{s}{x_1 x_2 \cdots x_n} = m. \tag{6.3}$$

If there were an infinite number of solutions to (6.3), at least one has some $|x_i| \geq 6|s|$. For this solution $|\frac{s}{x_1 x_2 \cdots x_n}| \leq \frac{1}{3}$, so that

$$|R| \leq \sum_{i=1}^{n} \frac{1}{|x_i|} \leq (n-1) + \frac{1}{6|s|} \leq n - \frac{5}{6}.$$

However (6.3) gives

$$|R| \geq |m| - |\frac{s}{x_1 x_2 \cdots x_n}| \geq |m| - \frac{1}{6}.$$

Combining these yields $|m| \leq n - \frac{2}{3} < n$, so $|m| \leq n-1$.

It remains to treat the cases $m = \pm(n-1)$. If $|m| = (n-1)$, and $|x_{n-2}| > 1$, then $|R| < n - 2 + \frac{1}{2} + \frac{1}{6|s|} \leq n - \frac{4}{3}$, while (6.3) gives $|R| \geq (n-1) - \frac{|s|}{6|s|} = n - \frac{7}{6}$, a contradiction. Thus we must have all $|x_i| = 1$ for $1 \leq i \leq n-2$. For the case $m = n-1$, we must have all these $x_i = 1$ and (6.1) simplifies to

$$\frac{1}{x_n} - \frac{s}{x_n} = 0.$$

This has infinitely many solutions if and only if $s = 1$. For the case $m = -(n-1)$, all $x_i = -1$ for $1 \leq i \leq n-1$ and (6.1) simplifies to

$$\frac{1}{x_n} - (-1)^{n-1}\frac{s}{x_n} = 0.$$

This equation has infinitely many integer solutions if and only if $s = (-1)^{n-1}$.

Sufficiency. We choose $x_n = \pm 1$ so that $sgn(x_n) = sgn(m)$. In that case the equation becomes

$$\left(\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_{n-1}}\right) - sgn(m)\frac{s}{x_1 x_2 \cdots x_{n-1}} = sgn(m)(|m| - 1). \tag{6.4}$$

By multiplying this equation by $sgn(x_n)$ we then get an equation of the same form with one fewer variable, with $s' = sgn(m)s$, and with a right side decreased by one in absolute value.

Continuing in this way, since $|m| \leq n-1$, we eventually arrive at a system with $n' = n - |m|$ variables and right hand side value $m' = 0$. For $n' = 1$ the system is of the form

$$\frac{1}{x_1} - \frac{s'}{x_1} = 0,$$

(where $s' = \pm s$) which has infinitely many solutions if and only if $s' = 1$. This corresponds to the two cases above.

For $n' = 2$, it has the form

$$\frac{1}{x_1} + \frac{1}{x_2} - \frac{s'}{x_1 x_2} = 0$$

These have the infinite family of solutions, for $m > |s'| + 2$, $(x_{,1}, x_2) = (m, -(m - s'))$ if $s' > 0$, and $(x_1, x_2) = (m, -(m + s'))$ if $s' < 0$. For $n' = 3$ it has the form

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} - \frac{s'}{x_1 x_2 x_3} = 0.$$

This has the family of solutions, for $m > |s'| + 2$ $(x_1, x_2, x_3) = (m, -(m+1), -m(m+1) - s')$ if $s' > 0$, $(x_1, x_2, x_3) = (-m, m+1, m(m-1) + s')$ if $s' < 0$.

The cases with $m = 0$ and $n \geq 4$ we can set two variables $x_n = 1, x_{n-1} = -1$ and reduce to an equation with two fewer variables and still with $m' = 0$. Continuing this way, we reduce to an equation (3.1) with $n = 2$ or $n = 3$ variables, having $m = 0$, which has infinitely many solutions by the constructions above. ∎

We now deduce Theorem 1.4.

Proof of Theorem 1.4. By hypothesis $r \geq 1$. We first show that $r = 1$ is a necessary condition for an infinite number of solutions. Indeed if $r \geq 2$, then we can eliminate variables $x_i = \pm 1$ and reduce to an equation with smaller n having all $|x_i| \geq 2$, with the same (r, s) values and a possibly different value of m, call it m'. But now Theorem 4.1 (1) rules out $m' = 0$, so we must have $m' \neq 0$. For $m' \neq 0$, Theorem 5.1 gives an upper bound on the size of the solutions which is independent of m', thus establishing finiteness in this case.

Suppose $r = 1$. Then the integer solutions to the affine equation (1.12) consist of solutions to (6.1) plus additional integer solutions having some variable $x_i = 0$. We show the solutions with $x_i = 0$ are finite in number. Indeed, if $x_n = 0$ then (1.12) simplifies in the remaining variables to

$$rx_1x_2 \cdots x_{n-1} + s = 0.$$

This clearly has finitely many solutions, since each $|x_i| \leq |s|$. The theorem now follows, using Theorem 6.1 to classify all cases when (6.1) has infinitely many integer solutions. ∎

References

[1] J. M. Borwein and E. Wong, A survey of results relating to Giuga's conjecture on primality, in: CRM Lecture Notes, Volume 11, Centre de Recherches Mathematiques, U. de Montreal, 1997, pp. 13-27.

[2] D. Borwein, J. M. Borwein, P. B. Borwein and R. Girgensohn, Giuga's conjecture on primality, Amer. Math. Monthly **103** (1996), 40–50.

[3] L. Brenton and R. Hill, On the Diophantine equation $1 = \sum \frac{1}{n_j} + \frac{1}{\prod n_j}$ and a class of homologically trivial complex surfaces, Pacific J. Math. **133** (1988), 41–67.

[4] D. R. Curtiss, On Kellogg's Diophantine problem, Amer. Math. Monthly **29** (1922), 380–387.

[5] P. Erdős, On the integer solutions to the equation $\frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n} = \frac{a}{b}$, (Hungarian) Math. Lapok, **1** (1950), 192–210. [MR 13, 208b].

[6] P. Erdős and R. L. Graham, *Old and new problems and results in combinatorial number theory*, Monographies de L'Enseignement Mathématiques, No. 28, Univ. de Genève, 1980.

[7] G. Giuga, Su una presumibile proprietà caratteristica dei numeri primi, Ist. Lombardo Sci. Lett. Rend. A **83** (1950), 511-528.

[8] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics, Second Edition* Addison-Wesley: Reading, Mass. 1994.

[9] D. Hensley, Lattice vertex polytopes with interior lattice points, Pacific J. Math. **105** (1983), 183–191.

[10] O. D. Kellogg, On a Diophantine problem, Amer. Math. Monthly **28** (1921), 300–303.

[11] J. C. Lagarias, G. M. Ziegler, Bounds for lattice polytopes containing a fixed number of interior points in a sublattice, Canadian J. Math. **43** (1991), 1022–1035.

[12] V. Nill, Volume and lattice points of reflexive simplices, Disc. Comp. Geom. **37** (2007), 301–320.

[13] A. Schinzel, Erdős's work on finite sums of unit fractions, in: (G. Halász, L. Lovász, M. Simonovits, V. Sós, Eds.) *Paul Erdős and His Mathematics I*, Springer: New York 2002, pp. 629–636.

[14] K. Soundararajan, Approximating 1 from below using n Egyptian fractions, eprint: `arXiv:math.CA/0502247`

[15] J. J. Sylvester, On a point in the theory of vulgar fractions, Amer. J. Math. **3** (1880) 332–335. Postscript to note on a point on vulgar fractions, ibid, 388–389.

[16] T. Takenouchi, On an indeterminate equation, Proc. Physico-Math. Soc. Japan (third series) **3** (1922), 78–92.

[17] J. Zaks, M. A. Perles and J. M. Wilks, On lattice polytopes having interior lattice points, Elem. Math. **37** (1982), 44–46.